REMARKS

In the Office Action dated April 7, 2006, claims 1-23 are pending. Claims 1, 8, 12-13, and 23 are independent claims from which all other claims depend therefrom. Claims 8, 10, 12-13, and 23 are herein amended for incidental reasons. Claim 11 is herein canceled. Claim 24 is newly added. Applicants respectfully request the Examiner for a reconsideration of the rejections.

The Office Action states that the claims remain rejected under 35 U.S.C. 112, second paragraph, but yet only provides arguments for claims 8 and 10-12. Applicants have closely reviewed the claims and have herein amended claims 8, 10, 12-13, and 23 and canceled claim 11. As a result of the amendments the issues with claim 12 are herein resolved. With respect to claims 8 and 10, claim 10 is herein amended to state that the user is authenticated by a policy engine within the privilege server, as opposed to referring to the authentication recited in claim 8. Claim 8 is herein amended to recite "user information" instead of "user identification." Applicants believe that the 35 U.S.C. 112 rejections are now overcome.

Claims 1-4 and 13-22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek (U.S. Pat. App. Pub. No. 2002/0095507) in view of Sampson (U.S. Pat. No. 6,490,624) and Lim (U.S. Pat. No. 6,728,884).

As well, Applicants note that Jerdonek, Sampson, and Lim are considered 102(e) type references, which are being combined and used in a 103(a) type rejection. Applicants submit that because only 102(e) type references support the 103(a) rejection, it would not have been obvious to combine the references at the time of the invention. Referring to MPEP 2136.02, the Supreme Court has authorized 35 U.S.C. 103 rejections based on a 35 U.S.C. 102(e) reference. The MPEP states that U.S. patents may be used as of their filing dates to show that the claimed subject matter is anticipated or obvious. The MPEP further states obviousness can be shown by combining **other** prior art with the U.S. patent reference in a 35 U.S.C. 103 rejection see *Hazeltine Research v. Brenner*, 382 U.S. 252, 147 USPQ 429 (1965). Thus, clearly it is appropriate to combine a 102(e) type

reference with another type of prior art reference in a 103 rejection. The MPEP does not state that it is appropriate to combine solely 102(e) references in a 103 rejection. This is also evident in review of *Hazeltine* in which a 102(e) reference was combined with another reference that issued prior to the application in issue in *Hazeltine*.

Applicants submit that the Jerdonek, Sampson, and Lim references were inaccessible to the Applicants at the time of filing of the present application. The Patent Office holds applications in secret and inaccessible to others until the publishing and/or issuance thereof. In this case, Jerdonek, Sampson, and Lim all issued and/or were published after the filing of the present application. Thus, Applicants submit that it would not have been obvious or even possible to combine the stated references to arrive at the claimed invention. For this reason alone, the 35 U.S.C. 103(a) rejections of the Office Action are overcome. Additional reasons are provided below.

Applicants note that the Examiner relies heavily on Jerdonek for disclosing all of the limitations of claims 1-4 and 13-22 except the forming of a packet at a privilege server, the validating of a user at a service server, and the privileges being role based.

Applicants submit that not only does Jerdonek fail to teach or suggest the stated limitations, but Jerdonek also fails to teach or suggest several of the other claimed limitations.

The Office Action states that Jerdonek discloses the limitations of presenting user information to the web adaptor from the user privilege server proxy, presenting user information to a head end server, and presenting user information to a privilege server from a head end server and refers to paragraphs 45, 46, and 63 of Jerdonek. In paragraphs 45, 46, and 63, user information is not provided. In the stated paragraphs, Jerdonek discloses a client system requesting a one-time password. No user information is provided in obtaining the one-time password. Although the system of Jerdonek, in paragraph 44, discloses a user entering items such as user name, PIN, and biometric data, this information is supplied to the client system for self-authentication. This information is not supplied to a server. Note that the steps performed for the self-

authentication are performed prior to the client system contacting the external server or any other server.

The Office Action then states that Jerdonek discloses validating the user in response to the user information and refers to paragraph 47 of Jerdonek. The Office Action states that there is some validation due to the password being pre-authorized. In paragraph 47, Jerdonek discloses a one-time or pre-authorization password, which is generated in response to the request for a one-time password. The one-time password is not activated and is provided to the client system as a challenge. The one-time password is provided for pre-authorization of the client. The one-time password is not pre-authorized and is clearly not authorized based on client information. It is the job of the client system to decrypt the one-time password to generate a proper digital signature. Pre-authorization is based on whether the digital signature is correct. When correct the one-time password is activated. The generation of the one-time password and the generation of the digital signature are not based on user information. Thus, the claimed validation is not taught or suggested.

The Office Action states that Jerdonek discloses forming a service access request token from a ticket and user information. Applicants, respectfully, disagree. The Office Action compares the claimed ticket and token to the one-time password and digital signature, respectively, of Jerdonek. Although the claimed ticket may contain a password or password information, it clearly also contains other information. Thus, it is unclear to Applicants how the formation of a digital signature from a one-time password is the same as the generation of a token from a ticket. Nevertheless, the digital signature of Jerdonek is clearly not formed from user information, as described above. The digital signature is a transformation of the one-time password with a private key. See paragraph 49 of Jerdonek.

The Office Action further states that Jerdonek discloses the limitations of forming a packet having a sequence number, a session key, and a ticket, providing the packet to a head end server, authenticating a user at a head end server in response to the packet,

and providing the packet to the user privilege server proxy and refers to paragraphs 45, 46, 56, and 63. Note that the stated limitations, as claimed, are performed after the generation of a ticket. The relied upon paragraphs refer to the initial challenge or the request and generation of the one-time password or the like. The stated paragraphs do not refer to a packet, and clearly a packet that has a ticket is not the same as a one-time password. Besides, nowhere in the stated paragraphs or anywhere else in Jerdonek is a sequence number or a session key mentioned or disclosed. The term "sequence" is not used anywhere in Jerdonek. Although Jerdonek discloses private, public, and domain keys, such keys are not session keys. Private keys are associated with, for example, a particular user. Public keys are associated with multiple users. Domain keys are associated with a certification authority. Private keys, public keys, and domain keys are used for multiple or many different sessions. On the other hand, session keys are each associated with a particular session or a communication interchange over a particular time period. Also, notice that not only are the claimed elements of a packet not disclosed in Jerdonek, that the term "packet" and the like is not mentioned anywhere in Jerdonek. As such, the limitations that recite a packet and the reception and transfer of a packet are not taught or suggested in Jerdonek.

The Office Action then states that Jerdonek discloses the sending of a ticket and a sequence number encrypted with a session key to a service server through a web adaptor. As stated above, Jerdonek fails to disclose a sequence number or a session key. Also, there is no suggestion in Jerdonek for the encryption of a ticket and a sequence number using a session key. Thus, Jerdonek fails to teach or suggest many of the limitations of claim 1 and 13.

The Office Action states that Sampson discloses forming a packet at a privilege server and refers to the Abstract of Sampson. Applicants are unsure as to what in the Abstract of Sampson the Examiner is referring. Applicants are unable to find anywhere in the Abstract the mention of a packet or the formation of a packet by a privilege server. The Abstract refers to a session manager that determines whether a client is

involved in an authenticated session with an access server and based thereon allows that client to access a protected server. The session manager is not part of the protected server and does not generate a packet. Also, the tasks performed by the protected server are not mentioned in the Abstract. The protected server of Sampson does not form a packet and especially not as claimed.

The Office Action also states that Lim discloses validating a user at a service server and refers to col. 8, lines 16-33 of Lim. In the stated section, Lim refers to an authentication method that is performed by a remote security server, which is accessed by an authentication and authorization module 114 via a proxy security server. Both the proxy security server and the remote security server are not service servers. The proxy security server and the remote security server are used solely for security purposes and are not used to provide a desired client service. The proxy security server and the remote security server simply provide information that specifies whether a user is authenticated and the access roles of that user. In addition, the authorization module 114 is not a server and is not part of a server, but rather is used as a security manager to access the appropriate proxy security server. Moreover, note that the access server 106 of Lim does not validate a user, since this is performed by the proxy security server and the remote security server.

Applicants also, submit that the architectures of Jerdonek, Sampson, and Lim are substantially different. It is unclear to the Applicants how the stated references would be combined. Also, no motivation has been provided to combine and modify the stated references as is necessary to arrive at the claimed invention. Thus, it would not have been obvious to make such a combination.

Like Jerdonek, Sampson and Lim, also fail to teach or suggest many of the limitations recited in claims 1 and 13. Sampson and Lim do not disclose the necessary servers, as required by claims 1 and 13. As such, Sampson and Lim do not teach or suggest the presenting of user information, the generation of a ticket, token, and packet, the sending of information to a service server, or the validating of a user via a service

server, as claimed. Referring to MPEP 706.02(j) and 2143, to establish a *prima facie* case of obviousness the prior art reference(s) must teach or suggest all the claim limitations, see *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Thus, since Jerdonek, Sampson, and Lim alone or in combination fail to teach or suggest each and every element of claims 1 and 13, Applicants submit that claim 1 and 13 are novel, nonobvious, and are in a condition for allowance. Since claims 2-4 and 14-22 depend from claim 13, they are also novel, nonobvious, and are in a condition for allowance for at least the same reasons.

Claims 5-12 and 23 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek in view of Sampson and Lim, and further in view of Menezes et al., "Handbook of Applied Cryptography", 1997, pp. 15-21 and 31.

The Office Action states that Jerdonek, Sampson, and Lim disclose the method of claim 1, in addition, Jerdonek discloses that the data is a ticket and refers to paragraph 47 of Jerdonek. Applicants have shown above that Jerdonek, Sampson, and Lim fail to teach or suggest many of the limitations of claim 1. Also, paragraph 47 of Jerdonek does not disclose that data is a ticket, but rather discloses the generation of a one-time password and does not refer to data or a ticket.

The Office Action states that Jerdonek, Sampson, and Lim fail to disclose the limitation of encrypting data with a user password to form an encrypted data. Applicants agree. The Office Action relies on Menezes for such teaching. Applicants submit that Menezes fails to disclose a password, the use of a password, or the encryption of data with a password.

Menezes simply discloses different encryption techniques, see page 15, lines 15-17. For example, Menezes discloses and describes symmetric-key encryption and mentions public-key encryption. Neither of these encryption techniques utilizes a password or is based off of a password. As described in Menezes, symmetric-key encryption takes an English message transforms it into groups of five letters and applies a permutation to each letter. Public-key encryption although not described in Menezes,

is another form of encryption, which is not password based. Menezes also describes different classes of encryption, which are referred to as ciphers. Ciphers are also different types of encryption techniques, which are also not password based. For example, a block cipher is a class of symmetric-key encryption, which breaks up plain text into strings of fixed length over an alphabet and encrypts one block at a time.

Thus, all of the relied upon references fail to teach or suggest the limitation of encrypting a ticket with a user password to form an encrypted ticket. As a result, any limitations that are performed in response to, as a result of, or post the encryption of the ticket, such as: providing the encrypted ticket to the user privilege server proxy through the head end server; decrypting the encrypted ticket to form a decrypted ticket; forming a service access request token from the decrypted ticket and the user information at the user privilege server proxy; sending the token from the user privilege server proxy to the privilege server; validating the user in response to the token; forming a packet having a sequence number and session key encrypted with the ticket at the privilege server; providing the packet to the head-end server; in response to the packet, authenticating the user at the head end server; providing the packet to the user privilege server proxy; decrypting the packet; sending the ticket and sequence number encrypted with the session key to a service server through the web adapter; validating the user at the service server; and granting the user role based privileges at the service server, are also not taught or suggested by the relied upon references. Therefore, the relied upon references fail to teach or suggest each and every element of claims 5-12 and 23.

Claim 8 also recites the limitation of negotiating an authentication scheme between a user privilege server proxy and a privilege server. The Office Action states that Lim provides such teaching. Applicants submit that there is not authentication scheme negotiated between the protected servers 104 of Lim and a user privilege server proxy. There is not any authentication scheme negotiated with the protected servers 104 or between any two devices. Rather, in Lim, authentication is performed by the

remote security servers 140 and communicated to the authentication and authorization module 114. In the Office Action referred to section of Lim, col. 5, lines 18-44, Lim merely discloses that the access system 100 that has the remote security servers 140 is used to allow users to log in and access resources on a network. Nowhere in the stated section is an authentication scheme negotiated with the networks 102 or the protected servers 104.

Besides, as stated above it is improper to combine 35 U.S.C. 102(e) type references in a 35 U.S.C. 103(a) rejection.

In light of the above remarks, Applicants submit that all objections and rejections are now overcome. The application is now in condition for allowance and expeditious notice thereof is earnestly solicited. Should the Examiner have any questions or comments the Examiner is respectfully requested to call the undersigned attorney.

Please charge any fees required in the filing of this amendment to Deposit Account 50-0476.

Respectfully submitted,

ARTZ & ARTZ, PC

Jeffrey J. Chapp
Registration No. 50,579
28333 Telegraph Road, Suite 250
Southfield, MI 48034
(248) 223-9500

Date: July 7, 2006